

Notice of Allowability

Application No.

09/472,314

Applicant(s)

VASUDEVAN ET AL.

Examiner

Jenise E Jackson

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 8/20/2004.
2. ☒ The allowed claim(s) is/are 6-11, 20, 23-33 and 35-52.
3. ☐ The drawings filed on _____ are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 6. ☒ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☒ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date 1182005.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

Examiner's Statement

1. The Applicant is requested to submit a substitute specification, because there are hole punches in the current specification.
2. The Applicant is also requested to submit formal drawings.

Reasons For Allowance

3. Claims 6-11, 20, 23-33, 35-52 are allowable for the features of, “ using the stored results of the first key exchange processes to secure the traffic communication if the second key exchange processes are not successful because the client system becomes non-operational, and wherein the results of the first key exchange process are utilized even if a security parameter refresh timer has elapsed and no acknowledgment signal is received”. The reasons why the claims are allowable are listed below:

4. In the prior art of key exchange, prior art fails to disclose, “wherein the results of the first key exchange process are utilized even if a security parameter refresh timer has elapsed and no acknowledgment signal is received”. An example of prior art that fails to disclose the limitation of, “wherein the results of the first key exchange process are utilized even if a security parameter refresh timer has elapsed and no acknowledgment signal is received”, is Mamros. Mamros discloses the ISAKMP/Oakley protocol, in which keys are renegotiated periodically to maintain the security of the protected communication link. If the remote computer fails to respond to a re-key request, it is assumed that the computer is no longer reachable and the communications link and the associated security association are torn down. The security association disclosed in the prior art of key exchange and specifically the prior art of Mamros, is torn down when the timeout exception occurs. In prior art of key exchange, if the timeout has not occurred, and protected

Art Unit: 2131

keep alive message is sent to the remote computer, the remote computer must reply in order to keep communications open. If the remote computer does not respond to the keep alive message the local box assumes the remote computer is no longer reachable and tears down the security association. This differs from the claimed invention, that discloses, “wherein the results of the first key exchange process are utilized even if a security refresh timer has elapsed and no acknowledgement signal is received, because Mamros discontinues the secured communications between a local and remote box if the refresh timer(i.e. timeout), and no communication is received between the local and remote boxes, specifically the protected acknowledgement is not received in response to the keep alive message.

5. In regards to the limitation, “using the stored results of the first key exchange processes to secure the traffic communication if the second key exchange processes are not successful because the client system becomes non-operational”, is not disclosed in the prior art of key exchange. An example of prior art that does not disclose this is Mamros. Mamros, discloses that when the client is non-operational(i.e. does not respond to keep alive message) the connection is dropped/torn down. In Mamros, a new connection must be established in order to get a new key. This is in contrast, to prior art that discloses using the first key if the client is non-operational. Thus, prior art fails to disclose or suggest, using the stored results of the first key exchange processes to secure the traffic communication if the second key exchange processes are not successful because the client system becomes non-operational.

6. In the prior art of security, prior art fails to disclose, “wherein the results of the first key exchange process are utilized even if a security parameter refresh timer has elapsed and no acknowledgment signal is received”. An example of prior art that fails to disclose, this limitation

Art Unit: 2131

is Nikander. Nikander discloses an ISPEC engine that must deal with the security policy, the currently active security associations and the transforms between incoming and outgoing packets. The ISPEC engine must deal with the security association creation and expiration. Nikander discloses that a security association may have a limited lifetime defined by the amount of data transmitted using that security association. Further, Nikander discloses that the amount of data transmitted must be recorded and the transmission must be dropped or establishing process of a new security association must be initiated if the lifetime expires. This is in contrast, to the claimed limitation, that discloses, "wherein the results of the first key exchange process are utilized even if a security refresh timer has elapsed and no acknowledgement signal is received", because prior art of security discloses that the security association, key exchange have a limited lifetime(i.e. timer) and that when the time is up, and new security association must be requested. Thus prior art fails to disclose or suggest, the limitations above. Further, in the prior art of security, prior art fails to disclose using the stored results of the first key exchange processes to secure the traffic communication if the second key exchange processes are not successful because the client system becomes non-operational. An example of prior art that does not disclose this is Nikander. Nikander discloses that if the client is non-operational the key exchange processes is torn down. There is no suggestion or disclosure of using the first key exchange if the client is non-operational.

7. In the prior art of networking, prior art fails to disclose, "wherein the results of the first key exchange process are utilized even if a security parameter refresh timer has elapsed and no acknowledgment signal is received", is Boden. Boden discloses ISAKMP phase I and phase II connections. Boden discloses once a connection is created, filter rules and security association

Art Unit: 2131

are loaded into the stack in the kernel to protect the connection's traffic. Boden also discloses that keys are renegotiated. However, prior art of security fails to disclose or suggest, "wherein the results of the first key exchange process are utilized even if a security parameter refresh timer has elapsed and no acknowledgment signal is received".

8. Also in the prior art of networking, prior art fails to disclose using the stored results of the first key exchange processes to secure the traffic communication if the second key exchange processes to secure the traffic communication if the second key exchange processes are not successful, because the client system becomes non-operational, wherein the results of the first key exchange process are utilized even if a security parameter refresh timer has elapsed and non acknowledgment signal is received. An example of prior art that fails to disclose the limitations above is Hauser et al. Hauser discloses that the principal does not change the value of the new key until successful validation the CPW request. The new keys are not installed if a negative acknowledgement is sent. Hauser fails to disclose where the client is non-operational because the principal waits for acknowledgement from the workstation to change to the new key. Also, an acknowledgement is sent, a rejection is sent or acceptance. Hauser discloses an acknowledgement is sent in either case accept or reject. Thus, this is in contrast to the claimed limitation of prior art, that discloses using the stored results of the first key exchange processes to secure the traffic communication if the second key exchange processes to secure the traffic communication if the second key exchange processes are not successful, because the client system becomes non-operational, wherein the results of the first key exchange process are utilized even if a security parameter refresh timer has elapsed and non acknowledgment signal is received.

Art Unit: 2131

9. In the prior art of non-patent literature, prior art fails to teach, “wherein the results of the first key exchange process are utilized even if a security parameter refresh timer has elapsed and no acknowledgement signal is received”. An example of non-patent literature, that fails to teach this limitation is, Pekka Riikonen. Pekka Riikonen teaches that there are two phases of key exchange. Phase I and Phase 2. Pekka teaches that a re-key or key re-generation is a process where new key material is created for protecting IP traffic. Pekka teaches that the main cause of re-key in IPSEC is the expiration of the security association, which is to protect the traffic. The time when SA expires is dictated by the lifetime of the SA, which can be negotiated during phase I and Phase 2. Pekka teaches that the longer the same key is used, the more insecure the key becomes. Thus, non-patent literature, teaches away from the claimed limitation of, “wherein the results of the first key exchange process are utilized even if a security parameter refresh timer has elapsed and no acknowledgement signal is received”.

10. Also, in the prior art of non-patent literature, prior art fails to teach or suggest, using the stored results of the first key exchange processes to secure the traffic communication if the second key exchange processes are not successful, because the client system becomes non-operational. An example of prior art that fails to teach this limitation is RFC 2409. RFC 2409 teaches if an ISAKMP implementation is alerted that a SA will soon be needed, it can be replaced by an existing SA before the SA expires. There is no suggestion of non-patent literature, that suggest using the first key exchange if the client is non-operational.


Art Unit: 2131

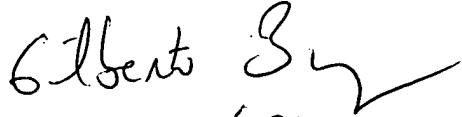
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


January 19, 2005


GILBERTO BARRÓN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100